DATA PROCESSING HARDWARE AND SOFTWARE

*** 1. **Purpose:** To provide policy for the use of state-owned data processing hardware and software. The office of primary responsibility for the DOT-OI is the Business Technology Support Division (BTSD). This DOT-OI supersedes DOT-OI 50-01 dated December 13, 2017.

2. **Hardware:**

A. State-owned mainframe computers, personal computers, mobile computing devices, printers, plotters, etc. will only be used by **authorized** personnel on official State business. Said personnel may include State employees, employees of other governmental entities, and employees of nongovernmental organizations working for the State.

B. The moving of data processing hardware (except laptop/notebook PC's) will be coordinated with the respective division/district head or BTSD Technical Services Section.

C. Using nonstate-owned or licensed hardware or software resources (i.e., networks, computers, software applications, etc.) for official State business is prohibited unless written approval is given by the appropriate Division Head/District Engineer and the BTSD Division Manager. No BTSD support will be provided for non-state-owned electronic telecommunication or technical resources.

D. The Nebraska Information Technology Commission (NITC) Standard 5-204 Linking a personal Portable Computing Device to the State Email System (http://nitc.ne.gov/standards/5-204.html) must be adhered to before final approval can be given. Adherence to this standard includes the signature and approval of the appropriate attachment to the standard. **These attachments include language authorizing possible impoundment of the device in the event of litigation.**

3. **Software:**

A. State-licensed/purchased software will be installed and used on state-owned hardware in accordance with the products license agreement.

B. Nonstate-licensed/purchased software may be installed and used on state-owned hardware if:

(1) Authorization is given by the division/district head or BTSD, **and**

(2) The BTSD Technical Services Section is notified of what is installed on what hardware, **and**

(3) It is not in violation of the software license agreement.

*** = Denotes changes made

C. Illegally copying software, either to or from state-owned hardware, is prohibited.

4. **Ownership:**

A. Data processing applications (programs, spreadsheets, etc.), created using state data processing resources or during working hours, are the sole property of the state.

B. Generally, the department will share application software, which it has the authority to distribute, with other governmental entities. The department will not share application software with private sector organizations except when:

(1) The organization is doing work for the department that requires the particular software application, or the organization agrees that the software will be used only on state or local highway, road, and street projects, **and**

(2) The organization agrees not to distribute the software product to any other organization, **and**

(3) The organization agrees not to change the software product without written authorization from the department, **and**

(4) The organization agrees that the department will be held blameless for the use of the software product.

C. Written approval by the division/district head in coordination with the BTSD is required for application software distributions.

5. **Security:**

A. The security of data and software resources on individual hardware or accessed through a network requires great care by authorized users. To that end, the following practices are prohibited.

(1) Automated "logons"

(2) Posting passwords or "logon" procedures in plain view.

B. The above practices can allow unauthorized personnel to access data and software resources with the risk potential ranging from nuisance to disaster. Therefore, if these practices are detected, the following steps will be taken.

(1) The "userid" will immediately be revoked.

(2) For the "userid" to be reinstated, the user's division/district head must send a signed letter to the BTSD Technical Services Section stating that the prohibited practice has stopped.

6. **Enforcement:** Personnel appointed by their division/district head, personnel from the BTSD, and personnel from department and other state audit staffs may, at any time, take measures to detect the improper use of state data processing resources.

7. **Violation:** Violators of this policy are subject to disciplinary action in accordance with the Nebraska Classified System Personnel Rules & Regulations, Chapter 14, "Disciplinary Action"; the Labor Contract Between the State of Nebraska and NAPE/AFSCME, Article 10, "Discipline or Investigatory Suspension"

***

Moe Jamshidi, P.E.
Deputy Director – Operations

ACCEPTABLE USE POLICY

*** 1. **Purpose:** Outline the acceptable use of electronic communication and technology resources at the Nebraska Department of Transportation (NDOT). These rules are in place to protect NDOT's employees, contractors, consultants, users, and the department from illegal or damaging actions by individuals, either knowingly or unknowingly. This policy is not meant to be inflexible concerning the use of NDOT electronic communication and technology resources. The intent is to create an environment where communications will flow freely and require a minimal amount of monitoring. NDOT divisions or districts may implement a division/district supplemental policy as long as it meets or exceeds the stipulations in this policy. This policy supersedes any previously issued Department policy regarding the use of NDOT electronic communication and technology. The office of primary responsibility for the DOT-OI is the Business Technology Support Division (BTSD). This DOT-OI supersedes DOT-OI 50-02 dated December 13, 2017.

2. **Definition:** Electronic communication and technology includes all devices used for voice or data communication.

3. **Scope:**

   A. This policy applies to employees, contractors, consultants, temporaries, and other workers at NDOT, including all personnel affiliated with third parties. This policy applies to all resources that are owned, leased, or used by NDOT including, but not limited to computer hardware, software, operating systems, data, storage media, networking equipment, telephones, and cellular equipment.

   B. This Acceptable Use Policy will be given to each current employee, and any new employee upon hire. Division Heads and District Engineers will assure that all employees receive a copy of this policy as well as other applicable electronic communication and technology standards and guidelines and sign the Acceptable Use Employee Agreement form. This form shall be permanently retained.

4. **Use and Responsibilities**

   General:

   A. NDOT employees should use electronic communication and technology resources for NDOT business only. Personal use of NDOT electronic communication and technology resources, including the use of the Internet and email, is to be kept to a minimum. NDOT management reserves the right to determine when an employee's use is excessive or improper.

   B. Electronic communication and technology resources that allow access to and use of the Internet and email are not to be used in a way that may be unlawful, disruptive, threatening, obscene, profane, offensive to others or harmful to morale. Use of the Internet, email and other actions must always be able to withstand public scrutiny without legal liability or embarrassment to the department.

*** = Denotes changes made

C. Employees may not use electronic communication and technology resources to solicit or petition others for commercial ventures, political or religious causes, outside organizations, or other non-job-related solicitations.

D. The unauthorized transmitting of sensitive Department information via electronic means is restricted. This includes, but is not limited to employee data, client, vendor, or contractor lists, bid information, credit card information, claims information, and software information.

Email:

A. Personal email should be sent and/or received as seldom, and be as brief, as possible. Because of limited storage space, any personal email must be deleted after being sent. Any personal email messages received should not be stored for an extended period of time. Personal email accounts outside of the Microsoft Outlook email system (i.e., Hotmail, Gmail, etc.) will not be accessed using electronic communication and technology resources.

B. NDOT prohibits the display or transmission of sexually explicit images, messages, or cartoons, or any transmission or use of e-mail communications that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement as defined by the Department of Transportation - Human Resources Workplace Harassment Policy and/or law.

Telecommunication Resources:

A. The only subscription allowed outside of basic service is weather service/alerts. Subscriptions to this feature are limited to district supervisory maintenance personnel with the prior written approval of the District Engineer and the Operations Division Manager.

B. The department will discontinue subscribing to text messaging services effective immediately and discourages receiving text messages because of the associated costs.

C. Non-exempt employees who are provided mobile devices should take calls and complete work during normal working hours. In the event that the employee must use their state-provided mobile device during non-working hours, the employee must be compensated accordingly and communicate that work time to their supervisor.

Use of Personal Equipment/Software with State-Owned Resources: Using non state-owned or licensed hardware or software resources (i.e., networks, computers, software applications, etc.) for official state business is prohibited unless written approval is given by the appropriate Division Head/District Engineer and the BTSD Division Manager. No BTSD support will be provided for non-state-owned electronic telecommunication or technical resources.

License Agreements: All electronic communication and technology users must abide by all software license agreements, copyright laws, trademark laws, patent laws, intellectual property laws, and applicable State and Federal laws.

Privacy: Information transmitted and/or stored on all electronic communication and technology resources is the sole property of the department. There is no right to privacy in any matter created, received, or sent and employees should not consider any information created or disseminated to be private. However, in those instances involving communication between a user and an attorney for the department, the communication should be clearly identified as "Privileged and Confidential, Attorney-Client Communication" and should identify the fact that the client is seeking legal advice to maintain the attorney-client privilege.

Electronic Communication and Technology Accounts and Passwords: All electronic communication and technology users must keep their accounts and passwords secure and are forbidden from sharing personal accounts or passwords. Authorized users are responsible for the security of their passwords, accounts, or systems and are responsible for any use or content associated with their account.

Security: Users of NDOT electronic communication and technology resources must not make any attempt to decode programs, access controlled files, crack passwords, monitor, scan or "sniff" the network, or use NDOT IS resources in any other way(s) to gain unauthorized access to data, information, networks or computers, whether owned or not owned by NDOT.

Enforcement: Authorized representatives of NDOT may periodically access and/or monitor the use of the electronic communication and technology resources. All e-mail messages, web pages, and other information flowing through or stored on electronic communication and technology resources is accessible to, and may be viewed or copied by, authorized NDOT representatives. Access and/or disclosure of another employee's files and messages without such employee's consent, except by an authorized employee of NDOT, is prohibited.

Violations: Employees found to be in violation of the above policies are subject to disciplinary action up to and including termination. Incidents of potential misuse will be reviewed and addressed on a case-by-case basis. Lack of knowledge of or familiarity with this policy shall not release an individual from such liability. The department reserves the right to inspect and monitor the electronic communication and technology resources for compliance at any time. The department reserves the right to terminate an employee's access to all or part of the electronic communication and technology at any time.

4. Questions regarding the terms or interpretation of this policy should be directed to the BTSD Division Manager or the Operations Division Manager as appropriate.

***

Moe Jamshidi, P.E.
Deputy Director – Operations

UNMANNED AIRCRAFT SYSTEMS (UAS)

*** 1. **Purpose:** To define the use of Unmanned Aircraft Systems (UAS) for the purposes of conducting Nebraska Department of Transportation (NDOT) business. The office of primary responsibility for this DOT-OI is the Business Technology Support Division (BTSD). This is a new DOT-OI dated September 23, 2019.

*** 2. **Background:** The use of UAS is expanding rapidly, as are the agencies using them. The Federal Aviation Administration has worked to standardize UAS policies and integrate unmanned aircraft into the National Airspace System (NAS). The Department is establishing the policy, roles and responsibilities, and procedures for operating UAS, as it relates to missions that are consistent with Department business.

*** 3. **Definitions**

*** A. **Certificate of Waiver or Authorization (COA):** An authorization issued by the FAA to grant NAS access for a specific UAS activity. COAs contain requirements the holder must follow. The FAA issues COAs for both public UAS operations and civil UAS operations.

*** B. **Flight:** An individual operation of the UAS from takeoff to landing. Each flight is required to have defined parameters for area of operation, altitudes, flight plan, and length of flight.

*** C. **Mission:** A mission normally has a specific purpose, timeframe, and defined location. A mission may require multiple flights.

*** D. **Pilot in Command (PIC):** A person who holds a pilot certificate with an UAS rating and has the final authority and responsibility for the operation and safety of an UAS operation conducted under Title 14 Code of Federal Regulations Part 107.

*** E. **Unmanned Aircraft (UA):** The flying portion of the system, flown by a pilot via a ground control system, or autonomously through use of an on-board computer, communication links, and any additional equipment that is necessary for the UA to operate safely.

*** F. **Unmanned Aircraft System (UAS):** The UA and all the associated support items such as equipment, control station, data links, telemetry, communications, and navigation equipment necessary to operate the unmanned aircraft.

*** G. **UAS Service Provider:** A consultant or other entity hired by NDOT to perform services within the scope of the UAS Use section of this policy.

*** H. **Visual Observer (VO):** A person acting as a member of a mission who assists the PIC to see and avoid obstacles.

*** = Denotes changes made

*** 4. **Policy**

*** A. **UAS Use:**

*** • UAS of a maximum gross takeoff weight of 55 pounds or less may be used when it provides cost efficiency, improved data quality, or improved personnel safety over an existing method or process. UAS use shall be for NDOT purposes. Examples of permitted uses include, but are not limited to, aerial photography, photogrammetry, bridge inspections, geotechnical field investigations, Light Detection and Ranging (LiDAR) applications, public outreach, documenting construction progress, mapping construction sites and conditions, asset management, asset inspections, traffic monitoring, incident management, disaster response, and training exercise.

*** • All flights will be conducted in accordance with and under the authority of Title 14 Code of Federal Regulations Part 107, a Section 333 Exemption and/or a Certificate of Authority (COA).

*** • Employees are prohibited from using privately owned UAS for Department business.

*** • Employees are prohibited from using Department UAS assets for private use.

*** • Employees operating agency-owned UAS will document compliance with FAA regulations, to include airworthiness of the UAS, licensing, aircraft registration, training, notifications and acquisition of all waivers and approvals prior to any UAS operation.

*** • Employees requiring assistance complying with Federal Aviation Administration (FAA) policies and Certificate of Waiver or Authorization (COA) process will consult with the UAS Program Manager.

*** • Aspects of this policy will not be construed as to restrict the safe, rapid deployment of an agency owned or contracted UAS in response to an emergency situation to protect life and limb, critical transportation infrastructure, or the environment.

*** B. **UAS Procurement:**

*** • The procurement of a Department owned UAS requires the approval of the Deputy Director or designee. The UAS Program Manager will coordinate the purchase to ensure the UAS equipment aligns with the mission needs.

*** • Procurement will be in accordance with applicable statutes, rules and Department Procurement policies and procedures.

*** C. **UAS Contracting Services:**

*** • Contracting for UAS services requires coordination with the UAS Program Manager, and a department template contract.

*** • UAS Service providers shall be required to obtain insurance coverage for bodily injury or property damage arising out of the ownership, maintenance, or use of any UAS owned or operated by the UAS Service provider with policy limits of at least $1,000,000 per occurrence.

*** D. **Operational and Training Requirements:**

*** • Employees and UAS Service Providers operating UAS will meet FAA UAS remote pilot or operator certification requirements (14 CFR Part 07).

*** • Employees require written approval from the UAS Program Manager in order to perform missions for NDOT.

*** • Flights will be logged and tracked by the PIC and include the date, time, location, and purpose of each flight.

*** E. **Safety Procedures:**

*** • Employees and UAS Service Providers operating an UAS will comply with FAA safety regulations, and any applicable state and local laws.

*** F. **Protection of Individual Privacy and Personal Information:**

*** • UAS operators will limit operations to the specific approved purpose of the mission and employ reasonable precautions to avoid capturing images of the public except those that are incidental to the project. Data collected on residential property cannot be the purpose of a mission unless pre-approved by the UAS Program Manager.

Moe Jamshidi, P.E.
Deputy Director - Operations